GOVERNMENT OF INDIA
HOME AFFAIRS
LOK SABHA

UNSTARRED QUESTION NO:115
ANSWERED ON:17.02.2009
CASES OF INTERNET FRAUD
Agarwal Shri Dhirendra;Kaushal Shri Raghuvir Singh;Renge Patil Shri Tukaram Ganpatrao

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether cases of Internet and Credit Card frauds are on the rise in the country;

(b) if so, the details thereof during each of the last three years and in the current year, State-wise including conviction rate achieved in such cases during the said period;

(c) whether the Central and State investigation agencies are fully equipped to deal with the such cases;

(d) if so, details of existing facilities available with the investigating agencies alongwith budgetary allocations made in the last three years and in the current year in this regard;

(e) if not, the reasons and constraints faced by the investigation agencies in dealing with such cases;

(f) whether the Government has any plan to increase the allocation for improving the facilities and training in Information Technology to personnel of the Central and State investigation agencies to effectively deal with such crimes;

(g) if so, details thereof and if not, reasons therefor;

(h) whether there is any need for strengthening the existing penal provisions relating to internet and credit card frauds; and

(i) if so, the details thereof alongwith details of steps being taken by the Government in this regard?

Answer

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS(DR. SHAKEEL AHMAD)

(a) & (b): The State-wise number of incidents of Internet frauds, i.e., cases of fraudulent withdrawal of money from banks through internet/online banking, as reported by the banks to the Reserve Bank of India (RBI), during the last three financial years and current year (upto December 2008) is at Annexure-I. RBI has intimated that the Credit Card frauds are reported by the issuing office of the bank, which is centralised in one city for each bank. Therefore, State-wise perpetration of Credit Card frauds is not reported to RBI. However, bank-wise data for Credit Card related frauds, as furnished by RBI, has been given at Annexure-II. The figures relating to the incidents of both Internet and Credit Card frauds indicate a mixed trend. RBI does not maintain data relating to conviction in such cases. Banks are required to report the matter to the State Police/CBI as per guidelines issued by RBI and pursue the cases with the investigative agencies till their logical end. However, as reported by the National Crime Records Bureau (NCRB), State/UT-wise details of cases registered under Fraud digital signature (Sec. 74 IT Act) and Breach of confidentiality / privacy (Sec 72 IT Act) and other related sections of IPC during 2005 to 2007 are enclosed at Annexure-III. The State/UT wise number of persons arrested during 2006 and 2007 in above offences are enclosed at Annexure-IV. Similar information for 2005 is not available. Other details regarding conviction are not maintained by NCRB.

(c): The Department of Information Technology (DIT) has set up Resource Centre for Cyber Forensics at the Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram, which has developed indigenous cyber forensics tools. These tools are now being used by agencies to investigate cyber crime cases. C-DAT, Thiruvananthapuram also conducts training programmes for law enforcement agencies on these tools. Organizations like Police Academies, Central Bureau of Investigation (CBI), Indian Computer Emergency Response Team (CERT-In), Controller of Certifying Authority (CCA), NCRB, Regional Police Computer Training Centres (RPCTCs) etc. conduct regular training programmes for imparting training to the police officials for preventing cyber crime in the country. The laboratories under the Directorate of Forensic Science (DFS) also conduct regular training programmes in the country for the benefit of law enforcement agencies and train them in search and seizure and handling of digital evidence. DIT has provided grants to CBI and Kerala Police to set up cyber forensics labs for investigation of cyber crimes and these labs will also be used for training the police officers. Therefore, it can be said that the Central and State investigation agencies are reasonably equipped to deal with such cases.

(d) to (g): The requisite information is being collected and would be laid on the Table of the House.

(h) & (i) The existing Information Technology Act, 2000 provides for legal framework to prevent cyber crimes including Internet frauds.Further, the Act has been amended to include provisions to address computer crimes like phising, spamming, online frauds

and identity theft as also for data protection. The Government has also conducted several awareness and training programmes on cyber laws and cyber crimes for Judicial Officers and law enforcement agencies.Indian Computer Emergency Response Team (CERT-In) under DIT provides reactive and proactive support to the cyber incidents in the country.It also liaisons with similar agencies worldwide and users of cyberspace in the country including Government, public or private and issues alerts, advisories and vulnerability notes.These advisories are also published on the website of CERT-IN (http://www.cert-in.org.in).CERT-IN also interacts with cyber users in the country to mitigate such incidents.